M thod and apparatus for encrypting and decrypting data using ncrypting k y contained in lectronic watermark

Patent Number: US2002108043
Publication date: 2002-08-08
Inventor(s): TANAKA NOBUYUKI (JP)
Applicant(s): NIPPON ELECTRIC CO (JP)
Requested Patent: JP2002232412
Application Number: US20020057521 20020124
Priority Number(s): JP20010027207 20010202
IPC Classification: H04L9/00
EC Classification: H04L9/08
Equivalents:

Abstract

In encoder side, an electronic watermark generating device generates an electronic watermark which contains a encryption key. An electronic watermark inserting device inserts the electronic watermark containing the encryption key into a first portion of data. An encrypting device encrypts a second portion of the data with the encryption key. The first portion into which the watermark containing the encryption key has been inserted and the second portion which has been encrypted with the encryption key are combined by a switch and thereafter recorded on a record medium or transmitted to a network. In decoder side, the watermark containing the encryption key is extracted from the first portion and the encryption key is extracted from the watermark. The second portion is decrypted with the extracted encryption key

(19)日本国特許庁(JP)　　(12)公開特許公報（Ａ）　　(11)特許出願公開番号

特開２００２－２３２４１２
（Ｐ２００２－２３２４１２Ａ）
(43)公開日　平成14年8月16日(2002.8.16)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｈ０４Ｌ	9/08		Ｇ０６Ｔ	1/00	５００　Ｂ	5B057
Ｇ０６Ｔ	1/00	５００	Ｇ０９Ｃ	5/00		5C063
Ｇ０９Ｃ	5/00		Ｇ１１Ｂ	20/10	Ｈ	5C064
Ｇ１０Ｌ	11/00		Ｈ０４Ｎ	1/387		5C076
	19/00		Ｈ０４Ｌ	9/00	６０１　Ｂ	5D044

審査請求　未請求　請求項の数７５　ＯＬ　（全２０頁）　最終頁に続く

(21)出願番号　特願2001-27207(P2001-27207)

(22)出願日　平成13年2月2日(2001.2.2)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目7番1号

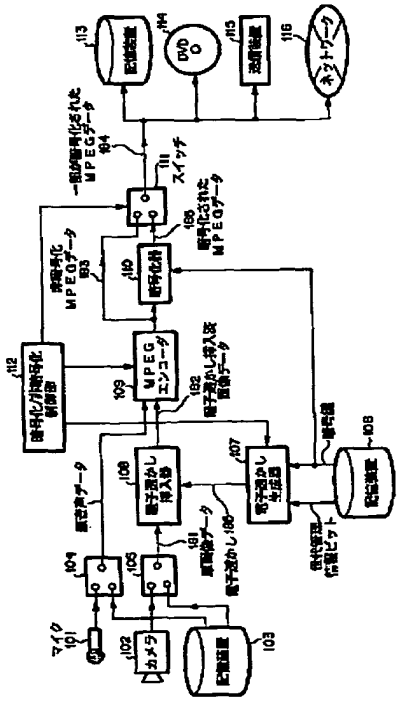
(72)発明者　田中　信行
東京都港区芝五丁目7番1号　日本電気株式会社内

(74)代理人　100065385
弁理士　山下　穣平

最終頁に続く

(54)【発明の名称】電子透かしに含めた暗号鍵を用いた暗号化装置及び復号化装置並びにそれらの方法

(57)【要約】
【課題】　電子透かし技術と、暗号化技術のそれぞれの特徴を活かし、それらを組み合わせることにより、よりセキュアなデジタルコンテンツの再生制限をすること可能とする。
【解決手段】　暗号化装置は、第１の暗号鍵を含んだ第１の電子透かしを生成する生成手段と、データの第１の部分に第１の暗号鍵を含んだ第１の電子透かしを挿入する電子透かし挿入手段と、データの第２の部分を第１の暗号鍵で暗号化する暗号化手段と、を備える。復号化装置は、データの第１の部分より第１の電子透かしを検出する電子透かし検出手段と、第１の電子透かしより第１の暗号鍵を抽出する暗号鍵抽出手段と、データの第２の部分を第１の暗号鍵で暗号解読する暗号解読手段と、を備える。



1

【特許請求の範囲】

【請求項１】　第１の暗号鍵を含んだ第１の電子透かしを生成する生成手段と、
データの第１の部分に前記第１の暗号鍵を含んだ前記第１の電子透かしを挿入する電子透かし挿入手段と、
前記データの第２の部分を前記第１の暗号鍵で暗号化する暗号化手段と、
を備えることを特徴とする電子透かしに含めた暗号鍵を用いた暗号化装置。

【請求項２】　請求項１に記載の暗号化装置において、
前記電子透かし生成手段は、第２の暗号鍵を含んだ第２の電子透かしを生成し、
前記電子透かし挿入手段は、前記第２の部分が前記暗号化手段により前記第１の暗号鍵で暗号化される前に、前記第２の部分に前記第２の電子透かしを挿入し、
前記暗号化手段は、前記データの第３の部分を前記第２の暗号鍵で暗号化することを特徴とする暗号化装置。

【請求項３】　請求項１に記載の暗号化装置において、
前記電子透かし生成手段は、第ｎ（ｎは１より大きい整数）の暗号鍵を含んだ第ｎの電子透かしを生成し、
前記電子透かし挿入手段は、第ｎの部分が前記暗号化手段により第（ｎ－１）の暗号鍵で暗号化される前に、前記第ｎの部分に前記第ｎの電子透かしを挿入し、
前記暗号化手段は、前記データの第（ｎ＋１）の部分を前記第ｎの暗号鍵で暗号化することを特徴とする暗号化装置。

【請求項４】　請求項１に記載の暗号化装置において、
前記データを圧縮する圧縮手段を更に備えることを特徴とする暗号化装置。

【請求項５】　請求項４に記載の暗号化装置において、
前記圧縮手段は、前記データを暗号化する前に、前記データを圧縮することを特徴とする暗号化装置。

【請求項６】　請求項１に記載の暗号化装置において、
前記データは画像データ、音声データ及び文字データの少なくとも１つを含むことを特徴とする暗号化装置。

【請求項７】　請求項１に記載の暗号化装置において、
前記第１の部分と前記第２の部分は同一の媒体に出力されることを特徴とする暗号化装置。

【請求項８】　請求項１に記載の暗号化装置において、
前記第２の部分は前記第１の部分と異なった媒体に出力されることを特徴とする暗号化装置。

【請求項９】　請求項１に記載の暗号化装置において、
前記第１の部分はコマーシャルを含むことを特徴とする暗号化装置。

【請求項１０】　データの第１の部分より第１の電子透かしを検出する電子透かし検出手段と、
前記第１の電子透かしより第１の暗号鍵を抽出する暗号鍵抽出手段と、
前記データの第２の部分を前記第１の暗号鍵で暗号解読する暗号解読手段と、

2

を備えることを特徴とする電子透かしに含めた暗号鍵を用いた復号化装置。

【請求項１１】　請求項１０に記載の復号化装置において、
前記電子透かし検出手段は、前記暗号解読手段により前記第１の暗号鍵で暗号解読された前記第２の部分より第２の電子透かしを検出し、
前記暗号鍵抽出手段は、前記第２の電子透かしより第２の暗号鍵を抽出し、
前記暗号解読手段は、前記データの第３の部分を前記第２の暗号鍵で暗号解読することを特徴とする復号化装置。

【請求項１２】　請求項１０に記載の復号化装置において、
前記電子透かし検出手段は、前記暗号解読手段により第（ｎ－１）（ｎは１より大きい整数）の暗号鍵で暗号解読された第ｎの部分より第ｎの電子透かしを検出し、
前記暗号鍵抽出手段は、前記第ｎの電子透かしより第ｎの暗号鍵を抽出し、
前記暗号解読手段は、前記データの第（ｎ＋１）の部分を前記第ｎの暗号鍵で暗号解読することを特徴とする復号化装置。

【請求項１３】　請求項１０に記載の復号化装置において、
前記データを伸長する伸長手段を更に備えることを特徴とする復号化装置。

【請求項１４】　請求項１３に記載の復号化装置において、前記伸長手段は、前記データが暗号解読された後に、前記データを伸長することを特徴とする復号化装置。

【請求項１５】　請求項１０に記載の復号化装置において、前記データは画像データ、音声データ及び文字データの少なくとも１つを含むことを特徴とする復号化装置。

【請求項１６】　請求項１０に記載の復号化装置において、前記第１の部分と前記第２の部分は同一の媒体から入力されることを特徴とする復号化装置。

【請求項１７】　請求項１０に記載の復号化装置において、前記第２の部分は前記第１の部分と異なった媒体から入力されることを特徴とする復号化装置。

【請求項１８】　請求項１０に記載の復号化装置において、前記第１の部分はコマーシャルを含むことを特徴とする復号化装置。

【請求項１９】　第１の暗号鍵を含んだ第１の電子透かしを生成するステップと、
データの第１の部分に前記第１の暗号鍵を含んだ前記第１の電子透かしを挿入するステップと、
前記データの第２の部分を前記第１の暗号鍵で暗号化するステップと、
を有することを特徴とする電子透かしに含めた暗号鍵を

用いた暗号化方法。

【請求項２０】　請求項１９に記載の暗号化方法において、

第２の暗号鍵を含んだ第２の電子透かしを生成するステップと、

前記第２の部分が前記第１の暗号鍵で暗号化される前に、前記第２の部分に前記第２の電子透かしを挿入するステップと、

前記データの第３の部分を前記第２の暗号鍵で暗号化するステップと、

を更に有することを特徴とする暗号化方法。

【請求項２１】　請求項１９に記載の暗号化方法において、

第ｎ（ｎは１より大きい整数）の暗号鍵を含んだ第ｎの電子透かしを生成するステップと、

第ｎの部分が前記暗号化手段により第（ｎ－１）の暗号鍵で暗号化される前に、前記第ｎの部分に前記第ｎの電子透かしを挿入するステップと、

前記データの第（ｎ＋１）の部分を前記第ｎの暗号鍵で暗号化するステップと、

を更に有することを特徴とする暗号化方法。

【請求項２２】　請求項１９に記載の暗号化方法において、

前記データを圧縮するステップを更に備えることを特徴とする暗号化方法。

【請求項２３】　請求項２２に記載の暗号化方法において、前記データを暗号化する前に、前記データを圧縮することを特徴とする暗号化方法。

【請求項２４】　請求項１９に記載の暗号化方法において、前記データは画像データ、音声データ及び文字データの少なくとも１つを含むことを特徴とする暗号化方法。

【請求項２５】　請求項１９に記載の暗号化方法において、

前記第１の部分を媒体に出力するステップと、

前記第２の部分を前記媒体と同一の媒体に出力するステップと、

を更に有することを特徴とする暗号化方法。

【請求項２６】　請求項１９に記載の暗号化方法において、

前記第１の部分を媒体に出力するステップと、

前記第２の部分を前記媒体と異なった媒体に出力するステップと、

を更に有することを特徴とする暗号化方法。

【請求項２７】　請求項１９に記載の暗号化方法において、前記第１の部分はコマーシャルを含むことを特徴とする暗号化方法。

【請求項２８】　データの第１の部分より第１の電子透かしを検出するステップと、

前記第１の電子透かしより第１の暗号鍵を抽出するステップと、

前記データの第２の部分を前記第１の暗号鍵で暗号解読するステップと、

を有することを特徴とする電子透かしに含めた暗号鍵を用いた復号化方法。

【請求項２９】　請求項２８に記載の復号化方法において、

前記第１の暗号鍵で暗号解読された前記第２の部分より第２の電子透かしを検出するステップと、

前記第２の電子透かしより第２の暗号鍵を抽出するステップと、

前記データの第３の部分を前記第２の暗号鍵で暗号解読するステップと、

を更に有することを特徴とする復号化方法。

【請求項３０】　請求項２８に記載の復号化方法において、

第（ｎ－１）（ｎは１より大きい整数）の暗号鍵で暗号解読された第ｎの部分より第ｎの電子透かしを検出するステップと、

前記第ｎの電子透かしより第ｎの暗号鍵を抽出するステップと、

前記データの第（ｎ＋１）の部分を前記第ｎの暗号鍵で暗号解読するステップと、

を更に有することを特徴とする復号化方法。

【請求項３１】　請求項２８に記載の復号化方法において、

前記データを伸長するステップを更に有することを特徴とする復号化方法。

【請求項３２】　請求項３１に記載の復号化方法において、前記データが暗号解読された後に、前記データを伸長することを特徴とする復号化方法。

【請求項３３】　請求項２８に記載の復号化方法において、前記データは画像データ、音声データ及び文字データの少なくとも１つを含むことを特徴とする復号化方法。

【請求項３４】　請求項２８に記載の復号化方法において、

前記第１の部分を媒体から入力するステップと、

前記第２の部分を前記媒体と同一の媒体から入力するステップと、

を更に有することを特徴とする復号化方法。

【請求項３５】　請求項２８に記載の復号化方法において、

前記第１の部分を媒体から入力するステップと、

前記第２の部分を前記媒体と異なった媒体から入力するステップと、

を更に有することを特徴とする復号化方法。

【請求項３６】　請求項２８に記載の復号化方法において、前記第１の部分はコマーシャルを含むことを特徴とする復号化方法。

【請求項３７】　第１の暗号鍵を含んだ第１の電子透かしを生成するステップと、
データの第１の部分に前記第１の暗号鍵を含んだ前記第１の電子透かしを挿入するステップと、
前記データの第２の部分を前記第１の暗号鍵で暗号化するステップと、
を有することを特徴とする電子透かしに含めた暗号鍵を用いた暗号化方法をコンピュータに実行させるためのコンピュータプログラム。
【請求項３８】　請求項３７に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
第２の暗号鍵を含んだ第２の電子透かしを生成するステップと、
前記第２の部分が前記第１の暗号鍵で暗号化される前に、前記第２の部分に前記第２の電子透かしを挿入するステップと、
前記データの第３の部分を前記第２の暗号鍵で暗号化するステップと、
を更に有することを特徴とするコンピュータプログラム。
【請求項３９】　請求項３７に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
第ｎ（ｎは１より大きい整数）の暗号鍵を含んだ第ｎの電子透かしを生成するステップと、
第ｎの部分が前記暗号化手段により第（ｎ－１）の暗号鍵で暗号化される前に、前記第ｎの部分に前記第ｎの電子透かしを挿入するステップと、
前記データの第（ｎ＋１）の部分を前記第ｎの暗号鍵で暗号化するステップと、
を更に有することを特徴とするコンピュータプログラム。
【請求項４０】　請求項３７に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
前記データを圧縮するステップを更に備えることを特徴とするコンピュータプログラム。
【請求項４１】　請求項４０に記載のコンピュータプログラムにおいて、前記暗号化方法は、前記データを暗号化する前に、前記データを圧縮することを特徴とするコンピュータプログラム。
【請求項４２】　請求項３７に記載のコンピュータプログラムにおいて、前記データは画像データ、音声データ及び文字データの少なくとも１つを含むことを特徴とするコンピュータプログラム。
【請求項４３】　請求項３７に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
前記第１の部分を媒体に出力するステップと、
前記第２の部分を前記媒体と同一の媒体に出力するステップと、
を更に有することを特徴とするコンピュータプログラム。
【請求項４４】　請求項３７に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
前記第１の部分を媒体に出力するステップと、
前記第２の部分を前記媒体と異なった媒体に出力するステップと、
を更に有することを特徴とするコンピュータプログラム。
【請求項４５】　請求項３７に記載のコンピュータプログラムにおいて、前記第１の部分はコマーシャルを含むことを特徴とするコンピュータプログラム。
【請求項４６】　データの第１の部分より第１の電子透かしを検出するステップと、
前記第１の電子透かしより第１の暗号鍵を抽出するステップと、
前記データの第２の部分を前記第１の暗号鍵で暗号解読するステップと、
を有することを特徴とする電子透かしに含めた暗号鍵を用いた復号化方法をコンピュータに実行させるためのコンピュータプログラム。
【請求項４７】　請求項４６に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
前記第１の暗号鍵で暗号解読された前記第２の部分より第２の電子透かしを検出するステップと、
前記第２の電子透かしより第２の暗号鍵を抽出するステップと、
前記データの第３の部分を前記第２の暗号鍵で暗号解読するステップと、
を更に有することを特徴とするコンピュータプログラム。
【請求項４８】　請求項４６に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
第（ｎ－１）（ｎは１より大きい整数）の暗号鍵で暗号解読された第ｎの部分より第ｎの電子透かしを検出するステップと、
前記第ｎの電子透かしより第ｎの暗号鍵を抽出するステップと、
前記データの第（ｎ＋１）の部分を前記第ｎの暗号鍵で暗号解読するステップと、
を更に有することを特徴とするコンピュータプログラム。
【請求項４９】　請求項４６に記載のコンピュータプログラムにおいて、
前記暗号化方法は、

前記データを伸長するステップを更に有することを特徴とするコンピュータプログラム。

【請求項５０】　請求項４９に記載のコンピュータプログラムにおいて、前記暗号化方法は、前記データが暗号解読された後に、前記データを伸長することを特徴とするコンピュータプログラム。

【請求項５１】　請求項４６に記載のコンピュータプログラムにおいて、前記データは画像データ、音声データ及び文字データの少なくとも１つを含むことを特徴とするコンピュータプログラム。

【請求項５２】　請求項４６に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
前記第１の部分を媒体から入力するステップと、
前記第２の部分を前記媒体と同一の媒体から入力するステップと、
を更に有することを特徴とするコンピュータプログラム。

【請求項５３】　請求項４６に記載のコンピュータプログラムにおいて、
前記暗号化方法は、
前記第１の部分を媒体から入力するステップと、
前記第２の部分を前記媒体と異なった媒体から入力するステップと、
を更に有することを特徴とするコンピュータプログラム。

【請求項５４】　請求項４６に記載のコンピュータプログラムにおいて、前記第１の部分はコマーシャルを含むことを特徴とするコンピュータプログラム。

【請求項５５】　第１の暗号鍵を含んだ第１の電子透かしを生成するステップと、
データの第１の部分に前記第１の暗号鍵を含んだ前記第１の電子透かしを挿入するステップと、
前記データの第２の部分を前記第１の暗号鍵で暗号化するステップと、
を有することを特徴とする電子透かしに含めた暗号鍵を用いた暗号化方法をコンピュータに実行させるためのコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項５６】　請求項５５に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
第２の暗号鍵を含んだ第２の電子透かしを生成するステップと、
前記第２の部分が前記第１の暗号鍵で暗号化される前に、前記第２の部分に前記第２の電子透かしを挿入するステップと、
前記データの第３の部分を前記第２の暗号鍵で暗号化するステップと、
を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項５７】　請求項５５に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
第ｎ（ｎは１より大きい整数）の暗号鍵を含んだ第ｎの電子透かしを生成するステップと、
第ｎの部分が前記暗号化手段により第（ｎ－１）の暗号鍵で暗号化される前に、前記第ｎの部分に前記第ｎの電子透かしを挿入するステップと、
前記データの第（ｎ＋１）の部分を前記第ｎの暗号鍵で暗号化するステップと、
を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項５８】　請求項５５に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
前記データを圧縮するステップを更に備えることを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項５９】　請求項５８に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、前記暗号化方法は、前記データを暗号化する前に、前記データを圧縮することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６０】　請求項５５に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、前記データは画像データ、音声データ及び文字データの少なくとも１つを含むことを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６１】　請求項５５に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
前記第１の部分を媒体に出力するステップと、
前記第２の部分を前記媒体と同一の媒体に出力するステップと、
を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６２】　請求項５５に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
前記第１の部分を媒体に出力するステップと、
前記第２の部分を前記媒体と異なった媒体に出力するステップと、

を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６３】　請求項５５に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、前記第１の部分はコマーシャルを含むことを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６４】　データの第１の部分より第１の電子透かしを検出するステップと、
前記第１の電子透かしより第１の暗号鍵を抽出するステップと、
前記データの第２の部分を前記第１の暗号鍵で暗号解読するステップと、
を有することを特徴とする電子透かしに含めた暗号鍵を用いた復号化方法をコンピュータに実行させるためのコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６５】　請求項６４に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
前記第１の暗号鍵で暗号解読された前記第２の部分より第２の電子透かしを検出するステップと、
前記第２の電子透かしより第２の暗号鍵を抽出するステップと、
前記データの第３の部分を前記第２の暗号鍵で暗号解読するステップと、
を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６６】　請求項６４に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
第（ｎ－１）（ｎは１より大きい整数）の暗号鍵で暗号解読された第ｎの部分より第ｎの電子透かしを検出するステップと、
前記第ｎの電子透かしより第ｎの暗号鍵を抽出するステップと、
前記データの第（ｎ＋１）の部分を前記第ｎの暗号鍵で暗号解読するステップと、
を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６７】　請求項６４に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
前記データを伸長するステップを更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６８】　請求項６７に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、前記暗号化方法は、前記データが暗号解読された後に、前記データを伸長することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６９】　請求項６４に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、前記データは画像データ、音声データ及び文字データの少なくとも１つを含むことを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項７０】　請求項６４に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
前記第１の部分を媒体から入力するステップと、
前記第２の部分を前記媒体と同一の媒体から入力するステップと、
を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項７１】　請求項６４に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記暗号化方法は、
前記第１の部分を媒体から入力するステップと、
前記第２の部分を前記媒体と異なった媒体から入力するステップと、
を更に有することを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項７２】　請求項６４に記載のコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体において、前記第１の部分はコマーシャルを含むことを特徴とするコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項７３】　第１の暗号鍵を含んだ第１の電子透かしが挿入された第１の部分と、
前記第１の暗号鍵により暗号化された第２の部分と、
を有するデータが記録されたコンピュータ読み取り可能な記録媒体。

【請求項７４】　請求項７３に記載のコンピュータ読み取り可能な記録媒体において、
前記第２の部分には、第２の暗号鍵を含んだ第２の電子透かしが挿入され、
前記データは、前記第２の暗号鍵により暗号化された第３の部分を有することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項７５】　請求項７３に記載のコンピュータ読み取り可能な記録媒体において、
前記第ｎ（ｎは１より大きい整数）の部分には、第ｎの暗号鍵を含んだ第ｎの電子透かしが挿入され、

前記データは、前記第ｎの暗号鍵により暗号化された第（ｎ＋１）の部分を有することを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタルデータに電子透かしを挿入する方法及び装置並びにデジタルデータから電子透かしを検出する方法及び装置に関し、特に、デジタル画像データに電子透かしを挿入する方法及び装置並びにデジタル画像データから電子透かしを検出する方法及び装置に関する。

【０００２】また、本発明はデジタルデータを暗号化する方法及び装置並びに暗号化されたデジタルデータを復号する方法及び装置に関し、特に、デジタル画像データを暗号化する方法及び装置並びに暗号化されたデジタル画像データを復号する方法及び装置に関する。

【０００３】

【従来の技術】近年、画像データや音声データは、デジタル化されてから蓄積、伝送、配布等がされるようになってきた。一方、デジタル化に伴うデータの違法な複製が大きな問題となっている。電子透かしデータの挿入・検出技術は、そのような違法な複製を防止する技術として注目を浴びており、実現化に向けて検討が進んでいる。また、電子透かしデータとは別にデータやプログラム等の改竄を防ぐ技術として暗号化方式がある。これは、データやプログラム自体をある暗号キーにより暗号化し、その暗号キーがなければそのデータやプログラムがデータやプログラムとして成り立たないようにする技術である。

【０００４】

【発明が解決しようとする課題】しかし、暗号化技術は、一度その暗号キーを解読されてしまうと、暗号化したデータも簡単にアクセスできてしまうと言う弱点があり、ＤＶＤ(Digital Versatile Disk)に施されているＣＳＳ(Contents Scrambling System)のように、同一の暗号鍵（単一の暗号鍵又は１組の暗号鍵）で全てのＤＶＤコンテンツを暗号化した場合、その暗号鍵を解読されると、全てのＤＶＤコンテンツの暗号を解いて、不正にコピー出来てしまうと言うことになる。

【０００５】そこで、各コンテンツをコンテンツ毎の暗号鍵を用いて暗号化することによりＣＳＳの問題点を解決できる。しかし、暗号鍵をコンテンツとは別のルートでＤＶＤの購買者に送付すると、購買者はコンテンツ毎に異なった暗号鍵を再生機又は再生ソフトに設定しなければならず、購買者の操作が煩わしい。また、暗号鍵をＭＰＥＧ(Moving Picture Experts Group)データの特定の領域に挿入すると、不正者が容易にＭＰＥＧデータから暗号鍵を抜き取り、抜き取った暗号鍵により暗号化されていないＭＰＥＧデータを取り出し、暗号化されていないＭＰＥＧデータを複製することが可能となってしまう。

【０００６】特開平１１－３１７８５９号公報に記載の技術は、電子透かしを画像データに挿入すると共に、電子透かしをスクランブルのための座標変換データの一部として使用して、画像ブロック単位で画像をスクランブルすることにより、再生側で、画像データに挿入された電子透かしと同一の電子透かしを用意している場合に限り、スクランブルを解除できるようにしたものである。しかし、この技術では、画像データの暗号化が行われておらず、画像ブロック単位でスクランブルが行われているだけであるので、スクランブルを解かなくても、どのフレームからも電子透かしを検出することができ、電子透かしを隠蔽することが全く出来ない。また、画像データを圧縮しようとした際、画像ブロック単位でスクランブルが行われているので、空間の連続性が無くなり、画像ブロックの動きベクトルを検出できず、動き補償フレーム間予測符号化を用いることが出来なくなってしまい、従って、高能率に圧縮することが出来なくなってしまう。

【０００７】そこで、本発明では電子透かし技術と、暗号化技術のそれぞれの特徴を活かし、よりセキュアなデジタルコンテンツの再生制限をすることを可能とする、電子透かしに含めた暗号鍵を用いた暗号化装置及びその方法並びに電子透かしに含めた暗号鍵を用いた復号化装置及びその方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明の第１の観点によれば、第１の暗号鍵を含んだ第１の電子透かしを生成する生成手段と、データの第１の部分に前記第１の暗号鍵を含んだ前記第１の電子透かしを挿入する電子透かし挿入手段と、前記データの第２の部分を前記第１の暗号鍵で暗号化する暗号化手段と、を備えることを特徴とする電子透かしに含めた暗号鍵を用いた暗号化装置が提供される。

【０００９】上記の暗号化装置において、前記電子透かし生成手段は、第２の暗号鍵を含んだ第２の電子透かしを生成し、前記電子透かし挿入手段は、前記第２の部分が前記暗号化手段により前記第１の暗号鍵で暗号化される前に、前記第２の部分に前記第２の電子透かしを挿入し、前記暗号化手段は、前記データの第３の部分を前記第２の暗号鍵で暗号化してもよい。

【００１０】上記の暗号化装置において、前記電子透かし生成手段は、第ｎ（ｎは１より大きい整数）の暗号鍵を含んだ第ｎの電子透かしを生成し、前記電子透かし挿入手段は、第ｎの部分が前記暗号化手段により第（ｎ－１）の暗号鍵で暗号化される前に、前記第ｎの部分に前記第ｎの電子透かしを挿入し、前記暗号化手段は、前記データの第（ｎ＋１）の部分を前記第ｎの暗号鍵で暗号化してもよい。

【００１１】上記の暗号化装置は、前記データを圧縮す

る圧縮手段を更に備えていてもよい。

【００１２】上記の暗号化装置において、前記圧縮手段は、前記データを暗号化する前に、前記データを圧縮してもよい。

【００１３】上記の暗号化装置において、前記データは画像データ、音声データ及び文字データの少なくとも１つを含んでいてもよい。

【００１４】上記の暗号化装置において、前記第１の部分と前記第２の部分は同一の媒体に出力されてもよい。

【００１５】上記の暗号化装置において、前記第２の部分は前記第１の部分と異なった媒体に出力されてもよい。

【００１６】上記の暗号化装置において、前記第１の部分はコマーシャルを含んでいてもよい。

【００１７】本発明の第２の観点によれば、データの第１の部分より第１の電子透かしを検出する電子透かし検出手段と、前記第１の電子透かしより第１の暗号鍵を抽出する暗号鍵抽出手段と、前記データの第２の部分を前記第１の暗号鍵で暗号解読する暗号解読手段と、を備えることを特徴とする電子透かしに含めた暗号鍵を用いた復号化装置が提供される。

【００１８】上記の復号化装置において、前記電子透かし検出手段は、前記暗号解読手段により前記第１の暗号鍵で暗号解読された前記第２の部分より第２の電子透かしを検出し、前記暗号鍵抽出手段は、前記第２の電子透かしより第２の暗号鍵を抽出し、前記暗号解読手段は、前記データの第３の部分を前記第２の暗号鍵で暗号解読してもよい。

【００１９】上記の復号化装置において、前記電子透かし検出手段は、前記暗号解読手段により第（ｎ－１）（ｎは１より大きい整数）の暗号鍵で暗号解読された第ｎの部分より第ｎの電子透かしを検出し、前記暗号鍵抽出手段は、前記第ｎの電子透かしより第ｎの暗号鍵を抽出し、前記暗号解読手段は、前記データの第（ｎ＋１）の部分を前記第ｎの暗号鍵で暗号解読してもよい。

【００２０】上記の復号化装置は、前記データを伸長する伸長手段を更に備えていてもよい。

【００２１】上記の復号化装置において、前記伸長手段は、前記データが暗号解読された後に、前記データを伸長してもよい。

【００２２】上記の復号化装置において、前記データは画像データ、音声データ及び文字データの少なくとも１つを含んでいてもよい。

【００２３】上記の復号化装置において、前記第１の部分と前記第２の部分は同一の媒体から入力されてもよい。

【００２４】上記の復号化装置において、前記第２の部分は前記第１の部分と異なった媒体から入力されてもよい。

【００２５】上記の復号化装置において、前記第１の部分はコマーシャルを含んでいてもよい。

【００２６】

【発明の実施の形態】以下、図面を参照して本発明の実施形態について詳細に説明する。

【００２７】［実施形態１］図１は、実施形態１による音声画像データ符号化装置及びその周辺部の構成を示すブロック図である。

【００２８】図１を参照すると、１０１は、音声を原音声データに変換するマイク、１０２は、画像を原画像データに変換するカメラ、１０３は、原音声データ及び原画像データを記憶している記憶装置、１０４は、マイク１０１からの原音声データ又は記憶装置からの原音声データを選択するスイッチ、１０５は、カメラ１０２からの原画像データ又は記憶装置１０３からの原画像データを選択し、原画像データ１８１を出力するスイッチである。

【００２９】１０６は、世代管理情報ビット及び暗号鍵を記憶する記憶装置、１０７は、世代管理情報ビット及び暗号鍵を基にこれらを含む電子透かしを生成する電子透かし生成器、１０８は、電子透かし生成器１０７が生成した電子透かし１８５をスイッチ１０５からの原画像データに挿入して、電子透かし挿入済画像データ１８２を生成する電子透かし挿入器である。

【００３０】１０９は、スイッチ１０４からの原音声データ及び電子透かし挿入器１０８からの電子透かし挿入済画像データを圧縮して非暗号化ＭＰＥＧデータ１８３を生成するＭＰＥＧエンコーダ、１１０は、ＭＰＥＧエンコーダ１０９からの非暗号化ＭＰＥＧデータを記憶装置１０６からの暗号鍵により暗号化して暗号化されたＭＰＥＧデータを生成する暗号化器、１１１は、ＭＰＥＧエンコーダ１０９からの非暗号化ＭＰＥＧデータ又は暗号化器１１０からの暗号化されたＭＰＥＧデータを選択して一部が暗号化されたＭＰＥＧデータ１８４を出力するスイッチである。

【００３１】なお、暗号化器１１０の行う暗号化は、例えば、ＤＥＳ(Data Encryption Standard)によるものであり、従って、暗号鍵は共通鍵である。

【００３２】１１２は、各時点で暗号化を行うか否かの制御を行う暗号化／非暗号化制御部であり、制御信号を電子透かし生成器１０７、ＭＰＥＧエンコーダ１０９、スイッチ１１１に出力する。

【００３３】スイッチ１１１から出力される一部が暗号化されたＭＰＥＧデータは、記憶装置１１３に記憶され、ＤＶＤ１１４に記録され、送信装置１１５から送信され、又は、ネットワーク１１６に送出される。送信装置１１５は、受信装置と対をなす送信装置のみならず放送局の放送用の送信装置も含む。

【００３４】図２は、図１に示す電子透かし挿入器１０８の構成を示すブロック図である。

【００３５】図２を参照すると、電子透かし挿入器１０

８は、離散コサイン変換器１２１、電子透かしデータ保持部１２２、挿入部１２３、逆離散コサイン変換器１２４を備える。

【００３６】離散コサイン変換器１２１は、空間領域の原画像データｘ（ｊ）に対して、例えば８画素×８画素の２次元の離散コサイン変換を行い、周波数領域の係数ｆ（ｉ）を出力する。ここで、ｊは、２次元から１次元に並べられた後の画素の番号を表し、ｉは、２次元から１次元に並べられた後の係数の番号を表す。

【００３７】電子透かしデータ保持部１２２は、電子透かしデータ

ｗ（１）、ｗ（２）、・・・、ｗ（ｎ）

を保持する。なお、電子透かしデータは平均０、分散１の正規分布に従う。

【００３８】挿入部１２３は、以下のことを行う。すなわち、係数ｆ（ｉ）と電子透かしデータｗ（ｉ）を基に、電子透かし挿入後の係数Ｆ（ｉ）を、

Ｆ（ｉ）＝ｆ（ｉ）＋α×ａｖｇ（ｆ（ｉ））×ｗ（ｉ）

の計算式により各ｉについて計算する。ここで、αはスケーリング要素であり、ａｖｇ（ｆ（ｉ））はｆ（ｉ）の近傍３点の絶対値の平均を取った部分平均である。そして、Ｆ（ｉ）を出力する。

【００３９】逆離散コサイン変換器１２４は、電子透かし挿入後の係数Ｆ（ｉ）に対して、逆離散コサイン変換を行い、空間領域の電子透かし挿入済画像データＸ（ｊ）を出力する。

【００４０】図３は、実施形態１による音声画像データ復号化装置及びその周辺部の構成を示すブロック図である。

【００４１】図３を参照すると、１４１は、送信装置１１４から送信されてきた一部が暗号化されたＭＰＥＧデータを受信する受信装置である。受信装置１４１は、送信装置と対をなす受信装置のみならず、放送局から送信されてきた放送を受信する受信装置も含む。

【００４２】１４２は、記憶装置１１３、ＤＶＤ１１４、受信装置１４１及びネットワーク１１６のうちの何れかからの一部が暗号化されたＭＰＥＧデータを選択するスイッチである。

【００４３】１４３は、一部が暗号化されたＭＰＥＧデータを入力し、各時点でそれが暗号化されているかいないかを検出する暗号化期間／非暗号化期間検出部であり、１４４は、一部が暗号化されたＭＰＥＧデータを入力し、暗号鍵抽出部１５４が電子透かしから抽出した暗号鍵を使用してその暗号を復号する暗号解読器、１４５は、暗号化／非暗号化検出部１４３からの暗号化期間／非暗号化期間検出信号に基づき、非暗号化期間では一部が暗号化されたＭＰＥＧデータを選択し、暗号化期間では暗号解読器１４４からの非暗号化ＭＰＥＧデータを選択するスイッチである。なお、スイッチ１４５が非暗号化期間で一部が暗号化されたＭＰＥＧデータを選択するときには、一部が暗号化されたＭＰＥＧデータは暗号化されていない。

【００４４】１４６は、非暗号化ＭＰＥＧデータを入力し、これを圧縮音声データと電子透かし挿入済圧縮画像データに分離して、これらを出力する画像／音声分離器、１４７は、圧縮音声データから音声データを復元する音声デーコーダ、１４８は、復元音声データを増幅してスピーカ駆動信号を生成する音声増幅器、１４９はスピーカ駆動信号を基に音声を出力するスピーカである。

【００４５】１５０は、電子透かし挿入済圧縮画像データから電子透かし挿入済復元画像データを復元する画像デコーダ、１５１は、電子透かし挿入済復元画像データを基にディスプレイ駆動信号を生成するディスプレイ駆動装置１５１、１５２は、ディスプレイ駆動信号を基に画像を表示するディスプレイである。

【００４６】１５３は、電子透かし挿入済復元画像データから電子透かしを検出して、電子透かしを暗号解読器１４４に出力する電子透かし検出部、１５４は、電子透かしから暗号鍵を抽出し、暗号鍵を出力する暗号鍵抽出部、１５５は、電子透かしから世代管理情報ビットを抽出し、世代管理情報ビットを出力する世代管理情報ビット抽出部である。

【００４７】世代管理情報ビットは、２ビットで表され、その値により、コピー・フリー(copy free)、コピー・ワンス(copy once)又はコピー禁止(inhibit)を示し、コピーマーク、メディアの種類の情報との組み合わせにより再生禁止、コピー禁止のために用いられるが、本発明の範囲外であるので、その説明は省略する。

【００４８】図４は、図３に示す電子透かし検出器１５３の構成を示すブロック図である。

【００４９】図４を参照すると、電子透かし検出器１５３は、離散コサイン変換器１６１、電子透かしデータ候補保持部１６２、検出部１６３を備える。

【００５０】離散コサイン変換器１６１は、空間領域の電子透かし挿入済画像データＸ（ｊ）に対して離散コサイン変換を行い、電子透かし挿入後の係数Ｆ（ｉ）を出力する。

【００５１】電子透かしデータ候補保持部１６２は、複数の電子透かしデータ候補を保持する。

【００５２】検出部１６３は、電子透かし挿入後の係数Ｆ（ｉ）を基に、電子透かしデータＷ（ｉ）を、

Ｗ（ｉ）＝Ｆ（ｉ）／ａｖｇ（Ｆ（ｉ））

の計算式により計算し、１フレーム分のＷ（ｉ）の総和ＷＦ（ｉ）を各ｉについて計算する。

【００５３】次に、検出部１６３は、電子透かし候補ｗ（ｉ）とＷＦ（ｉ）との統計的類似度Ｃをベクトルの内積を利用して、

Ｃ＝ＷＦ×ｗ／（ＷＦＤ×ｗＤ）

の計算式により計算する。ここで、

ＷＦ＝（ＷＦ（１）、ＷＦ（２）、・・・、ＷＦ（ｎ））、
ｗ＝（ｗ（１）、ｗ（２）、・・・、ｗ（ｎ））、
ＷＦＤ＝ベクトルＷＦの絶対値、
ｗＤ＝ベクトルｗの絶対値
である。統計的類似度Ｃがある特定の値以上である場合には、該当電子透かしデータが埋め込まれていると判定する。

【００５４】図５は、実施形態１による音声画像データ符号化装置の各部が出力する信号を示す図であり、スイッチ１０５が出力する原画像データ１８１、電子透かし挿入器１０８が出力する電子透かし挿入済画像データ１８２、ＭＰＥＧエンコーダ１０９が出力する非暗号化ＭＰＥＧデータ１８３、スイッチ１８４が出力する一部が暗号化されたＭＰＥＧデータ１９４を示す。

【００５５】図５を参照すると、電子透かし挿入済画像データ１８２に挿入される電子透かし１８５は、８ビットより構成され、符号１８５－１で示すように、非暗号化期間では、２ビットの世代管理情報ビットと６ビットの暗号鍵より構成され、符号１８５－２で示すように、暗号化期間では２ビットの世代管理情報ビットと任意の値を取る６ビットより構成される。なお、図５の例では、世代管理情報ビットは、”１１(binary)”の値を取り、これは、コピー禁止を示す。

【００５６】１つの電子透かしには、６ビットの暗号鍵しか入れられないが、暗号鍵を分割して、複数の電子透かしに分散して挿入することにより、６ビットよりもビット数が多い暗号鍵を電子透かしとして画像データに挿入することができる。例えば、１５フレームに１つの電子透かしを挿入することができるので、ＮＴＳＣ方式であれば、約２秒間に２４ビットの暗号鍵を画像データに挿入することができる。但し、電子透かしを挿入した後の画質を考慮して、２秒よりも長い時間に２４ビットの暗号鍵を挿入するようにしても良い。

【００５７】一部が暗号化されたＭＰＥＧデータ１８４は、符号１８４－１で示すように、非暗号化期間では、暗号化されず、符号１８４－２で示すように、暗号化期間では、暗号化される。

【００５８】なお、暗号化期間及び非暗号化期間のＭＰＥＧデータへの割当は、ファイル毎に行っても良いし、シーケンス毎に行っても良い。また、ＭＰＥＧデータのプライベート・パケットに暗号化期間／非暗号化期間を示すフラグを挿入したり、非暗号化期間を固定時間とすれば、暗号化期間及び非暗号化期間のＭＰＥＧデータへの割当をファイル毎又はシーケンス毎に行わなくても良い。

【００５９】図６は、実施形態１による音声画像データ符号化装置の主要な部分の動作を示すタイミング図である。

【００６０】図６を参照すると、非暗号化期間では、電子透かし生成器１０７は、暗号鍵を含む電子透かし１８５－１を生成し、電子透かし挿入器１０８は、原画像データに電子透かし１８５－１を挿入し、ＭＰＥＧエンコーダ１０９は、電子透かし挿入済画像データに対しＭＰＥＧエンコードを行い、スイッチ１１１は、ＭＰＥＧエンコーダ１０９からの非暗号化ＭＰＥＧデータ１８３を選択する。なお、暗号化器１１０は、非暗号化期間では、非暗号化ＭＰＥＧデータの暗号化を行わない。

【００６１】暗号化期間では、電子透かし生成器１０７は、暗号鍵を含まない電子透かし１８５－２を生成し、電子透かし挿入器１０８は、原画像データに電子透かし１８５－２を挿入し、ＭＰＥＧエンコーダ１０９は、電子透かし挿入済画像データに対しＭＰＥＧエンコードを行い、暗号化器１１０は非暗号化ＭＰＥＧデータを非暗号化期間で電子透かしに含めた暗号鍵で暗号化し、スイッチ１１１は、暗号化されたＭＰＥＧデータ１８５を選択する。

【００６２】図７は、実施形態１による音声画像データ復号化装置の主要な部分の動作を示すタイミング図である。

【００６３】図７を参照すると、非暗号化期間では、暗号化期間／非暗号化期間検出部１４３は、一部が暗号化されたＭＰＥＧデータが暗号化されているか否かを検出する。検出の方法は、ファイル毎に暗号化期間及び非暗号化期間がＭＰＥＧデータへ割当てられているか、シーケンス毎に暗号化期間及び非暗号化期間がＭＰＥＧデータへ割当てられているか、ＭＰＥＧデータのプライベート・パケットに暗号化期間／非暗号化期間を示すフラグを挿入されているか、又は、非暗号化期間を固定時間とされているかにより異なる。

【００６４】また、非暗号化期間では、画像／音声分離器１４６は、非暗号化ＭＰＥＧデータを圧縮音声データと電子透かし挿入済圧縮画像データに分離し、音声デコーダ１４７は、圧縮音声データより音声データを復元し、画像デコーダ１５０は、電子透かし挿入済圧縮画像データより電子透かし挿入済画像データを復元し、電子透かし検出部１５３は、電子透かし挿入済画像データより世代管理情報ビットと暗号鍵を含む電子透かしを検出し、暗号鍵抽出部１５４は、電子透かしより暗号鍵を抽出し、世代管理情報ビット抽出部１５５は、電子透かしより世代管理情報ビットを抽出し、スイッチ１４５は、暗号解読器１４４が入力する一部が暗号化されたＭＰＥＧデータと同一のデータを選択する。非暗号化期間では、一部が暗号化されたＭＰＥＧデータは暗号化されていない。

【００６５】なお、非暗号化期間では暗号解読器１４４は、暗号の解読を行わない。

【００６６】暗号化期間では、暗号化期間／非暗号化期間検出部１４３は、一部が暗号化されたＭＰＥＧデータが暗号化されているか否かを検出し、暗号解読器１４４

は、暗号化されたＭＰＥＧデータの暗号を非暗号化期間で暗号鍵抽出部１５４が電子透かしより抽出した暗号鍵を用いて解読し、画像／音声分離器１４６は、非暗号化ＭＰＥＧデータを圧縮音声データと電子透かし挿入済圧縮画像データに分離し、音声デコーダ１４７は、圧縮音声データより音声データを復元し、画像デコーダ１５０は、電子透かし挿入済圧縮画像データより電子透かし挿入済画像データを復元し、電子透かし検出部１５３は、電子透かし挿入済画像データより世代管理情報ビットを含む電子透かしを検出し、世代管理情報ビット抽出部１５５は、電子透かしより世代管理情報ビットを抽出し、スイッチ１４５は、暗号解読器１４４が出力する非暗号化ＭＰＥＧデータを選択する。

【００６７】なお、暗号化期間では、暗号鍵抽出部１５４は、電子透かしより暗号鍵を抽出しない。

【００６８】実施形態１によれば、以下の効果が奏される。

【００６９】１つのコンテンツの暗号鍵が見破られても、その暗号鍵により他のコンテンツの暗号を解読することが出来ないので、コンテンツ制作者の著作権を厚く保護することができる。また、１つのコンテンツを複数の部分に分割した上で実施形態１を適用した場合には、１つの部分の暗号鍵が見破られても、その暗号鍵により他の部分の暗号鍵を解読することが出来ないので、コンテンツ制作者の著作権を厚く保護することができる。

【００７０】暗号鍵がコンテンツ内に含まれているので、視聴者が暗号鍵をコンテンツと別ルートで入手し、再生機に設定する必要がなくなる。

【００７１】暗号鍵がそのままの形でＭＰＥＧデータに挿入されていないので、暗号鍵をＭＰＥＧデータから抜き出すことが困難になる。特に、再生装置を暗号鍵抽出部が出力する暗号鍵を外部からアクセスすることを防止できるような構造とすることにより、不正者が暗号鍵を抜き出すことが不可能となる。

【００７２】再生装置は、電子透かし検出器を有さなければ、音声及び画像を再生することが出来ないので、電子透かし検出器を有しない海賊版の再生装置で、音声及び画像を再生することが出来ない。

【００７３】暗号鍵を含む電子透かしが挿入されている画像データを再生しなければ、暗号化されている画像データの暗号を復号することが出来ないので、例えば、コマーシャルに暗号鍵を含む電子透かしを挿入することにより、視聴者が必ずコマーシャルを視聴することになり、従って、コンテンツ制作者はスポンサーからの収益源を確保することが出来る。

【００７４】［実施形態２］実施形態２は、ＭＰＥＧデータのうちの第１の暗号鍵により暗号化された第１の暗号化期間の電子透かしに第２の暗号鍵を含ませ、その第２の暗号鍵によりＭＰＥＧデータのうちの他の部分を暗号化し、このような暗号化の連鎖を繰り返すものである。すなわち、暗号化期間を複数の暗号化期間に分割し、それぞれの暗号化期間のＭＰＥＧデータを他の暗号化期間の電子透かしに含まれている暗号鍵により暗号化するものである。

【００７５】実施形態２による音声画像データ符号化装置の構成は、図１に示す実施形態１による音声画像データ符号化装置と同一であるので、その説明は省略する。また、実施形態２による音声画像データ復号化装置の構成は、図３に示す実施形態１による音声画像データ復号化装置と同一であるので、その説明も省略する。

【００７６】図８は、実施形態２による音声画像データ符号化装置の各部が出力する信号を示す図であり、スイッチ１０５が出力する原画像データ１８１、電子透かし挿入器１０８が出力する電子透かし挿入済画像データ１８２、ＭＰＥＧエンコーダ１０９が出力する非暗号化ＭＰＥＧデータ１８３、スイッチ１８４が出力する一部が暗号化されたＭＰＥＧデータ１９４を示す。

【００７７】図８を参照すると、電子透かし挿入済画像データ１８２に挿入される電子透かし１８５は、８ビットより構成され、符号１８５－３で示すように、非暗号化期間では、２ビットの世代管理情報ビットと６ビットの第１の暗号鍵より構成され、符号１８５－４で示すように、第１の暗号鍵による暗号化期間では、２ビットの世代管理情報ビットと６ビットの第２の暗号鍵より構成され、符号１８５－５で示すように、第２の暗号鍵による暗号化期間では、２ビットの世代管理情報ビットと６ビットの第３の暗号鍵より構成され、符号１８５－６で示すように、第３の暗号鍵による暗号化期間では２ビットの世代管理情報ビットと任意の値を取る６ビットより構成される。なお、図８の例では、図５の例と同様に、世代管理情報ビットは、”１１(binary)”の値を取り、これは、コピー禁止を示す。

【００７８】一部が暗号化されたＭＰＥＧデータ１８４は、符号１８４－３で示すように、非暗号化期間では、暗号化されず、符号１８４－４で示すように、第１の暗号鍵による暗号化期間（第１の暗号化期間）では、第１の暗号鍵により暗号化され、符号１８４－５で示すように、第２の暗号鍵による暗号化期間（第２の暗号化期間）では、第２の暗号鍵により暗号化され、符号１８４－６で示すように、第３の暗号鍵による暗号化期間（第３の暗号化期間）では、第３の暗号鍵により暗号化される。

【００７９】なお、第１乃至第３の暗号化期間及び非暗号化期間のＭＰＥＧデータへの割当は、ファイル毎に行っても良いし、シーケンス毎に行っても良い。また、ＭＰＥＧデータのプライベート・パケットに第１乃至第３の暗号化期間／非暗号化期間を示すフラグを挿入したり、第１乃至第３の暗号化期間及び非暗号化期間を固定時間とすれば、第１乃至第３の暗号化期間及び非暗号化期間のＭＰＥＧデータへの割当をファイル毎又はシーケ

ンス毎に行わなくても良い。

【００８０】図９は、実施形態２による音声画像データ符号化装置の主要な部分の動作を示すタイミング図である。

【００８１】図９を参照すると、非暗号化期間では、電子透かし生成器１０７は、第１の暗号鍵を含む電子透かし１８５－３を生成し、電子透かし挿入器１０８は、原画像データに電子透かし１８５－３を挿入し、ＭＰＥＧエンコーダ１０９は、電子透かし挿入済画像データに対しＭＰＥＧエンコードを行い、スイッチ１１１は、ＭＰＥＧエンコーダ１０９からの非暗号化ＭＰＥＧデータ１８３を選択する。なお、暗号化器１１０は、非暗号化期間では、非暗号化ＭＰＥＧデータの暗号化を行わない。

【００８２】第１の暗号化期間では、電子透かし生成器１０７は、第２の暗号鍵を含む電子透かし１８５－４を生成し、電子透かし挿入器１０８は、原画像データに電子透かし１８５－４を挿入し、ＭＰＥＧエンコーダ１０９は、電子透かし挿入済画像データに対しＭＰＥＧエンコードを行い、暗号化器１１０は非暗号化ＭＰＥＧデータを非暗号化期間で電子透かしに含めた第１の暗号鍵で暗号化し、スイッチ１１１は、暗号化されたＭＰＥＧデータ１８５を選択する。

【００８３】第２の暗号化期間では、電子透かし生成器１０７は、第３の暗号鍵を含む電子透かし１８５－５を生成し、電子透かし挿入器１０８は、原画像データに電子透かし１８５－５を挿入し、ＭＰＥＧエンコーダ１０９は、電子透かし挿入済画像データに対しＭＰＥＧエンコードを行い、暗号化器１１０は非暗号化ＭＰＥＧデータを第１の暗号鍵による暗号化期間で電子透かしに含めた第２の暗号鍵で暗号化し、スイッチ１１１は、暗号化されたＭＰＥＧデータ１８５を選択する。

【００８４】第３の暗号化期間では、電子透かし生成器１０７は、暗号鍵を含まない電子透かし１８５－６を生成し、電子透かし挿入器１０８は、原画像データに電子透かし１８５－６を挿入し、ＭＰＥＧエンコーダ１０９は、電子透かし挿入済画像データに対しＭＰＥＧエンコードを行い、暗号化器１１０は非暗号化ＭＰＥＧデータを第２の暗号鍵による暗号化期間で電子透かしに含めた第３の暗号鍵で暗号化し、スイッチ１１１は、暗号化されたＭＰＥＧデータ１８５を選択する。

【００８５】図１０は、実施形態２による音声画像データ復号化装置の主要な部分の動作を示すタイミング図である。

【００８６】図１０を参照すると、非暗号化期間では、暗号化期間／非暗号化期間検出部１４３は、一部が暗号化されたＭＰＥＧデータが暗号化されているか否かを検出する。検出の方法は、実施形態１と同様である。

【００８７】また、非暗号化期間では、画像／音声分離器１４６は、非暗号化ＭＰＥＧデータを圧縮音声データと電子透かし挿入済圧縮画像データに分離し、音声デコーダ１４７は、圧縮音声データより音声データを復元し、画像デコーダ１５０は、電子透かし挿入済圧縮画像データより電子透かし挿入済画像データを復元し、電子透かし検出部１５３は、電子透かし挿入済画像データより世代管理情報ビットと第１の暗号鍵を含む電子透かしを検出し、暗号鍵抽出部１５４は、電子透かしより第１の暗号鍵を抽出し、世代管理情報ビット抽出部１５５は、電子透かしより世代管理情報ビットを抽出し、スイッチ１４５は、暗号解読器１４４が入力する一部が暗号化されたＭＰＥＧデータと同一のデータを選択する。非暗号化期間では、一部が暗号化されたＭＰＥＧデータは暗号化されていない。

【００８８】なお、非暗号化期間では暗号解読器１４４は、暗号の解読を行わない。

【００８９】第１の暗号化期間では、暗号化期間／非暗号化期間検出部１４３は、一部が暗号化されたＭＰＥＧデータが暗号化されているか否かを検出し、暗号解読器１４４は、暗号化されたＭＰＥＧデータの暗号を非暗号化期間で暗号鍵抽出部１５４が電子透かしより抽出した第１の暗号鍵を用いて解読し、画像／音声分離器１４６は、非暗号化ＭＰＥＧデータを圧縮音声データと電子透かし挿入済圧縮画像データに分離し、音声デコーダ１４７は、圧縮音声データより音声データを復元し、画像デコーダ１５０は、電子透かし挿入済圧縮画像データより電子透かし挿入済画像データを復元し、電子透かし検出部１５３は、電子透かし挿入済画像データより世代管理情報ビット及び第２の暗号鍵を含む電子透かしを検出し、暗号鍵抽出部１５４は、電子透かしより第２の暗号鍵を抽出し、世代管理情報ビット抽出部１５５は、電子透かしより世代管理情報ビットを抽出し、スイッチ１４５は、暗号解読器１４４が出力する非暗号化ＭＰＥＧデータを選択する。

【００９０】第２の暗号化期間では、暗号化期間／非暗号化期間検出部１４３は、一部が暗号化されたＭＰＥＧデータが暗号化されているか否かを検出し、暗号解読器１４４は、暗号化されたＭＰＥＧデータの暗号を第１の暗号化期間で暗号鍵抽出部１５４が電子透かしより抽出した第２の暗号鍵を用いて解読し、画像／音声分離器１４６は、非暗号化ＭＰＥＧデータを圧縮音声データと電子透かし挿入済圧縮画像データに分離し、音声デコーダ１４７は、圧縮音声データより音声データを復元し、画像デコーダ１５０は、電子透かし挿入済圧縮画像データより電子透かし挿入済画像データを復元し、電子透かし検出部１５３は、電子透かし挿入済画像データより世代管理情報ビット及び第３の暗号鍵を含む電子透かしを検出し、暗号鍵抽出部１５４は、電子透かしより第３の暗号鍵を抽出し、世代管理情報ビット抽出部１５５は、電子透かしより世代管理情報ビットを抽出し、スイッチ１４５は、暗号解読器１４４が出力する非暗号化ＭＰＥＧデータを選択する。

【００９１】第３の暗号化期間では、暗号化期間／非暗号化期間検出部１４３は、一部が暗号化されたＭＰＥＧデータが暗号化されているか否かを検出し、暗号解読器１４４は、暗号化されたＭＰＥＧデータの暗号を第２の暗号化期間で暗号鍵抽出部１５４が電子透かしより抽出した第３の暗号鍵を用いて解読し、画像／音声分離器１４６は、非暗号化ＭＰＥＧデータを圧縮音声データと電子透かし挿入済圧縮画像データに分離し、音声デコーダ１４７は、圧縮音声データより音声データを復元し、画像デコーダ１５０は、電子透かし挿入済圧縮画像データより電子透かし挿入済画像データを復元し、電子透かし検出部１５３は、電子透かし挿入済画像データより世代管理情報ビットを含む電子透かしを検出し、世代管理情報ビット抽出部１５５は、電子透かしより世代管理情報ビットを抽出し、スイッチ１４５は、暗号解読器１４４が出力する非暗号化ＭＰＥＧデータを選択する。

【００９２】なお、第３の暗号化期間では、暗号鍵抽出部１５４は、電子透かしより暗号鍵を抽出しない。

【００９３】実施形態２によれば、実施形態１による効果に加え、以下の効果が奏される。

【００９４】暗号化期間を複数の暗号化期間に分割し、それぞれの暗号化期間のＭＰＥＧデータを他の暗号化期間の電子透かしに含まれている暗号鍵により暗号化しているので、暗号化期間全体の暗号を解くための暗号鍵を解読する時間が分割数に比例して増大する。従って、電子透かし検出器を有しない不正者が不正に暗号鍵を解読しようとする意欲を失わせることができる。また、不正に暗号鍵を解読して音声画像を停止無しに連続して再生することを防止することができる。

【００９５】［実施形態３］実施形態３を、その概念図である図１１を参照して説明する。

【００９６】非暗号化ＭＰＥＧデータ２０１は、記憶装置２０３に記憶されており、コンピュータ２０６からの要求に従い、記憶装置２０２からWWWサーバ２０４、インターネット等のネットワークを通じてコンピュータ２０６に伝送される。コンピュータに伝送された非暗号化ＭＰＥＧデータ２０１は、コンピュータの外部記憶装置等（不図示）に記憶される。WWWサーバ２０４からコンピュータ２０６への非暗号化ＭＰＥＧデータ２０１の伝送には、ＴＣＰ／ＩＰ(Transmission Control Protocol/Internet Protocol)上のＦＴＰ(file transfer protocol)等が用いられる。

【００９７】暗号化ＭＰＥＧデータ２０２は、ＤＶＤ等の可搬の記録媒体２０７に記録される。

【００９８】非暗号化ＭＰＥＧデータ２０１は、暗号化ＭＰＥＧデータに比べて、極めて小容量であり、これを記憶装置２０３からコンピュータ２０６に伝送する時間は、暗号化ＭＰＥＧデータを伝送する場合に比べて、極めて短い。また、非暗号化ＭＰＥＧデータ２０１には、暗号化ＭＰＥＧデータ２０２の暗号を解読するための暗号鍵が電子透かしの一部又は全部として挿入されている。更に、非暗号化ＭＰＥＧデータの画像内容は、暗号化ＭＰＥＧデータ２０２のコンテンツを示したり、その広告をしたりするものであることが好ましい。暗号化ＭＰＥＧデータ２０２は、非暗号化ＭＰＥＧデータ２０１に電子透かしの一部又は全部として含まれる暗号鍵により暗号化されている。

【００９９】使用者は、暗号化ＭＰＥＧデータ２０２のコンテンツを視聴しようとしたならば、コンピュータ２０６を操作することにより、記憶装置２０３に記憶されている非暗号化ＭＰＥＧデータ２０１をコンピュータ２０６にダウンロードして記憶させ、また、コンテンツ製造者から流通経路、店舗を介して記録媒体２０７を入手して、コンピュータ２０６にローディングする。コンピュータ２０６により実現される音声画像データ復号装置は、使用者からの操作に従い、まず、非暗号化ＭＰＥＧデータ２０１を再生し、この際に、電子透かしを検出し、検出された電子透かしから暗号鍵を抽出する。次に、コンピュータ２０６は、抽出された暗号鍵を用いて暗号を解読しながら暗号化ＭＰＥＧデータから音声画像を再生する。

【０１００】コンテンツ制作者は、コンピュータ２０６が非暗号化ＭＰＥＧデータをダウンロードする際に、暗号化ＭＰＥＧデータ２０２のコンテンツについて課金を行う。

【０１０１】なお、上記の実施形態３の説明では、音声画像データ復号装置はコンピュータにより実現されるとしたが、音声画像データ復号専用装置又は音声画像データ復号装置を兼ねた如何なる装置であっても良い。

【０１０２】また、上記の実施形態３の説明では、暗号化ＭＰＥＧデータ２０２はＤＶＤ等の可搬な記録媒体に記録されているとしたが、暗号化ＭＰＥＧデータ２０２が放送され、音声画像復号装置が暗号化ＭＰＥＧデータ２０２を受信して、外部記憶装置に記憶してから、再生するようにしても良い。

【０１０３】実施形態３によれば、コンテンツをネットワークをダウンロードするための時間を短縮することができる。また、非暗号化ＭＰＥＧデータ２０１をダウンロードするためのWWWサイトに広告を掲載することにより、コンテンツ制作者は、広告収入を得て、コンテンツの価格を下げることが可能となる。

【０１０４】［他の実施形態］実施形態３では、非暗号化ＭＰＥＧデータを通信によりコンテンツ事業者から消費者に配り、暗号化ＭＰＥＧデータをパッケージの形態でコンテンツ事業者から消費者に配るとしたが、非暗号化ＭＰＥＧデータ及び暗号化ＭＰＥＧデータは、それぞれ、コンテンツ事業者から消費者に通信により配られても良いし、パッケージの形態で配られても良いし、放送の形態で配られても良い。

【０１０５】実施形態１乃至３では、画像データに電子

透かしを挿入するとしたが、音声データ、文字データに電子透かしを挿入しても良い。実施形態１乃至３では、画像データ及び音声データを暗号化するとしたが、画像データのみ又は音声データのみを暗号化しても良い。また、文字データを暗号化しても良い。例えば、画像データの第１の部分に暗号鍵を含む電子透かしを挿入し、画像データの第２の部分のみを暗号化しても良いし、音声データの第１の部分に暗号鍵を含む電子透かしを挿入し、音声データの第２の部分のみを暗号化しても良いし、文字データの第１の部分に暗号鍵を含む電子透かしを挿入し、文字データの第２の部分のみを暗号化しても良い。また、画像データの第１の部分に暗号鍵を含む電子透かしを挿入し、画像データの第２の部分、音声データ及び文字データを暗号化しても良いし、音声データの第１の部分に暗号鍵を含む電子透かしを挿入し、音声データの第２の部分、画像データ及び文字データを暗号化しても良いし、文字データの第１の部分に暗号鍵を含む電子透かしを挿入し、文字データの第２の部分、画像データ及び音声データを暗号化しても良い。

【０１０６】実施形態２において、１つの長編のコンテンツを複数のＤＶＤに分割して収録し、１のＤＶＤに収録されているＭＰＥＧデータを他のＤＶＤに収録されているＭＰＥＧデータに挿入されている電子透かしに含まれる暗号鍵で暗号化するようにしてもよい。

【０１０７】図１に示す音声画像データ符号化装置及び図３に示す音声画像データ復号化装置は、それぞれ、必ずしもハードウェアにより実現されていなくても良い。すなわち、図１に示す音声画像データ符号化装置及び図３に示す音声画像データ復号化装置は、それぞれ、コンピュータを図１に示す音声画像データ符号化装置及び図３に示す音声画像データ復号化装置として機能させるためのプログラムをコンピュータが実行することによっても実現することができる。この場合、そのようなプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録されていることもあり、コンピュータがネットワークを介して他のコンピュータからダウンロードする場合もある。

【０１０８】実施形態１乃至３では、非暗号化ＭＰＥＧデータに電子透かしを挿入し、その電子透かしに暗号鍵を含め、その暗号鍵を用いて暗号化ＭＰＥＧデータの暗号を解読するようにしたが、必ずしも、暗号化ＭＰＥＧデータが暗号化されている必要はない。例えば、ＭＰＥＧデータを非隠蔽ＭＰＥＧデータと隠蔽ＭＰＥＧデータに分割し、非隠蔽ＭＰＥＧデータに電子透かしを挿入し、その電子透かしに隠蔽ＭＰＥＧデータの隠蔽を外すための隠蔽解除鍵を含め、その隠蔽解除鍵を用いて隠蔽ＭＰＥＧデータの隠蔽を外すようにしても良い。本発明では、このような隠蔽化も暗号化に含むものとし、隠蔽解除鍵も暗号鍵に含むものとする。

【０１０９】実施形態１乃至３では、音声画像圧縮方式としてＭＰＥＧデータを生成する方式を例に取り説明したが、他の方式であっても良い。また、音声画像の圧縮は省略しても良い。

【０１１０】

【発明の効果】以上説明したように、本発明によれば、以下の効果が奏される。

【０１１１】１つのコンテンツの暗号鍵が見破られても、その暗号鍵により他のコンテンツの暗号を解読することが出来ないので、コンテンツ制作者の著作権を厚く保護することができる。また、１つのコンテンツを複数の部分に分割した上で実施形態１を適用した場合には、１つの部分の暗号鍵が見破られても、その暗号鍵により他の部分の暗号鍵を解読することが出来ないので、コンテンツ制作者の著作権を厚く保護することができる。

【０１１２】暗号鍵がコンテンツ内に含まれているので、視聴者が暗号鍵をコンテンツと別ルートで入手し、再生機に設定する必要がなくなる。

【０１１３】暗号鍵がそのままの形でＭＰＥＧデータに挿入されていないので、暗号鍵をＭＰＥＧデータから抜き出すことが困難になる。特に、再生装置を暗号鍵抽出部が出力する暗号鍵を外部からアクセスすることを防止できるような構造とすることにより、不正者が暗号鍵を抜き出すことが不可能となる。

【０１１４】再生装置は、電子透かし検出器を有さなければ、音声及び画像を再生することが出来ないので、電子透かし検出器を有しない海賊版の再生装置で、音声及び画像を再生することが出来ない。

【０１１５】暗号鍵を含む電子透かしが挿入されている画像データを再生しなければ、暗号化されている画像データの暗号を復号することが出来ないので、例えば、コマーシャルに暗号鍵を含む電子透かしを挿入することにより、視聴者が必ずコマーシャルを視聴することになり、従って、コンテンツ制作者はスポンサーからの収益源を確保することが出来る。

【０１１６】暗号化期間を複数の暗号化期間に分割し、それぞれの暗号化期間のＭＰＥＧデータを他の暗号化期間の電子透かしに含まれている暗号鍵により暗号化しているので、暗号化期間全体の暗号を解くための暗号鍵を解読する時間が分割数に比例して増大する。従って、電子透かし検出器を有しない不正者が不正に暗号鍵を解読しようとする意欲を失わせることができる。また、不正に暗号鍵を解読して音声画像を停止無しに連続して再生することを防止することができる。

【図面の簡単な説明】

【図１】本発明の実施形態による音声画像データ符号化装置及びその周辺部の構成を示すブロック図である。

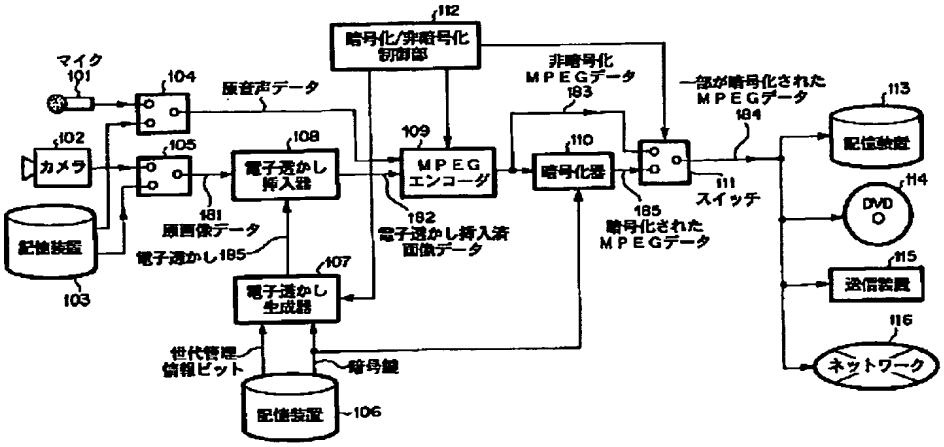
【図２】図１に示す電子透かし挿入器の一例の構成を示すブロック図である。

【図３】本発明の実施形態による音声画像データ復号化装置及びその周辺部の構成を示すブロック図である。

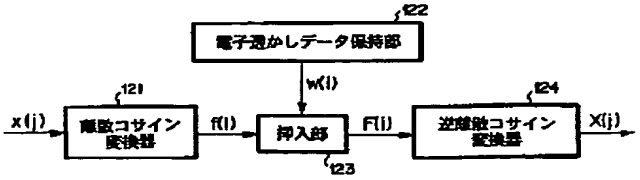
【図４】図３に示す電子透かし検出器の一例の構成を示

すブロック図である。
【図５】本発明の実施形態１による音声画像データ符号化装置の主要部が入出力するデータを示す図である。
【図６】本発明の実施形態１による音声画像データ符号化装置の主要部の動作を示すタイミング図である。
【図７】本発明の実施形態１による音声画像データ復号化装置の主要部の動作を示すタイミング図である。
【図８】本発明の実施形態２による音声画像データ符号化装置の主要部が入出力するデータを示す図である。
【図９】本発明の実施形態２による音声画像データ符号化装置の主要部の動作を示すタイミング図である。
【図１０】本発明の実施形態２による音声画像データ復号化装置の主要部の動作を示すタイミング図である。
【図１１】本発明の実施形態３を説明するための概念図である。
【符号の説明】
１０１　マイク
１０２　カメラ
１０３　記憶装置
１０４　スイッチ
１０５　スイッチ
１０６　記憶装置
１０７　電子透かし生成器
１０８　電子透かし挿入器
１０９　ＭＰＥＧエンコーダ
１１０　暗号化器
１１１　スイッチ
１１２　暗号化／非暗号以下制御部
１１３　記憶装置
１１４　ＤＶＤ
１１５　送信装置
１１６　ネットワーク
１４１　受信装置
１４２　スイッチ
１４３　暗号化期間／非暗号化期間検出器
１４４　暗号解読器
１４５　スイッチ
１４６　画像／音声分離器
１４７　音声デコーダ
１４８　音声増幅器
１４９　スピーカ
１５０　画像デコーダ
１５１　ディスプレイ駆動装置
１５２　ディスプレイ
１５３　電子透かし検出器
１５４　暗号鍵抽出部
１５５　世代管理情報ビット抽出部

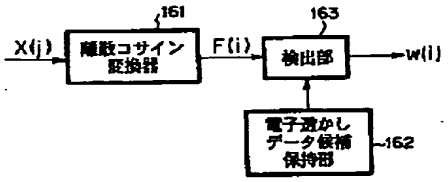
【図１】



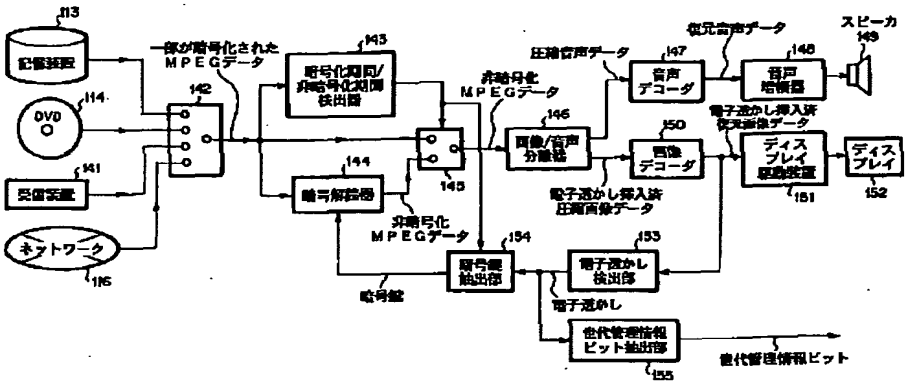
【図２】



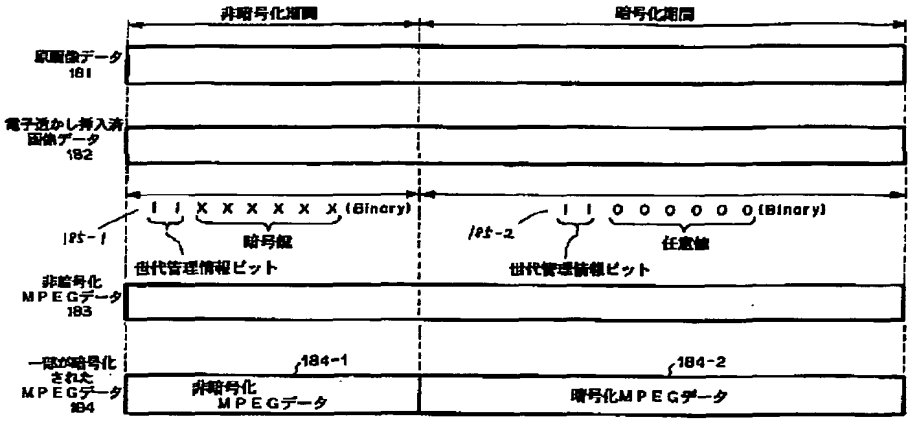
【図４】



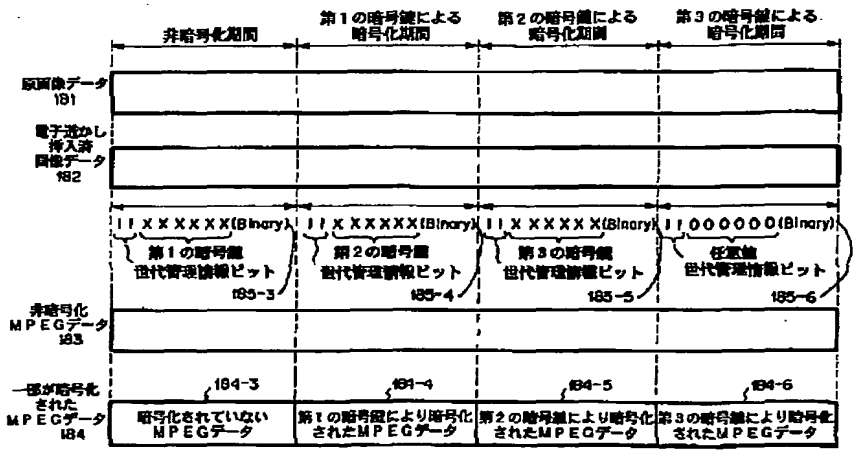
【図３】


113
記憶装置
DVD
114
141
受信装置
ネットワーク
116
一部が暗号化されたMPEGデータ
142
143
暗号化期間/非暗号化期間検出部
144
暗号解読部
145
非暗号化MPEGデータ
暗号鍵
146
画像/音声分離部
圧縮音声データ
147
音声デコーダ
復元音声データ
148
音声暗号器
スピーカ
149
150
画像デコーダ
電子透かし挿入済圧縮画像データ
電子透かし挿入済復元画像データ
ディスプレイ駆動装置
151
ディスプレイ
152
154
暗号鍵抽出部
153
電子透かし検出部
電子透かし
世代管理情報ビット抽出部
155
世代管理情報ビット

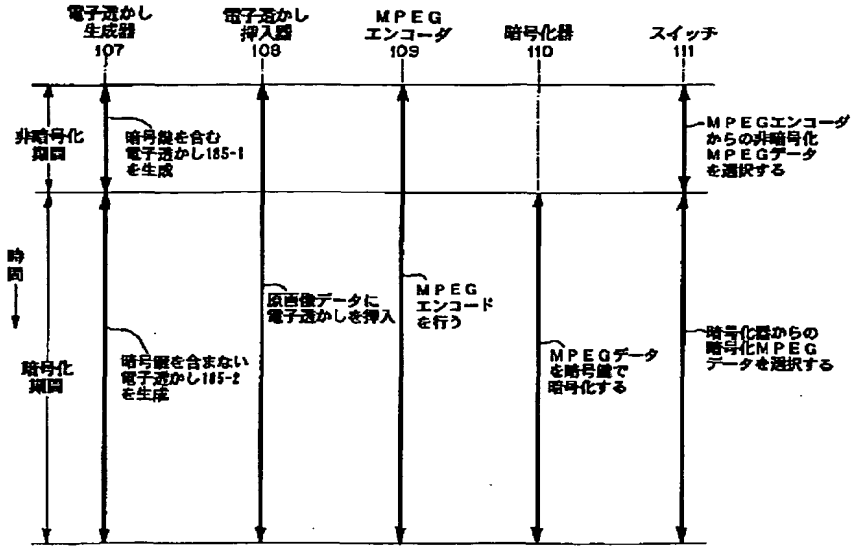
【図５】


非暗号化期間
暗号化期間
原画像データ 181
電子透かし挿入済画像データ 182
1 1 X X X X X X (Binary)
185-1
暗号鍵
世代管理情報ビット
1 1 0 0 0 0 0 0 (Binary)
185-2
任意値
世代管理情報ビット
非暗号化MPEGデータ 183
一部が暗号化されたMPEGデータ 184
184-1
非暗号化MPEGデータ
184-2
暗号化MPEGデータ

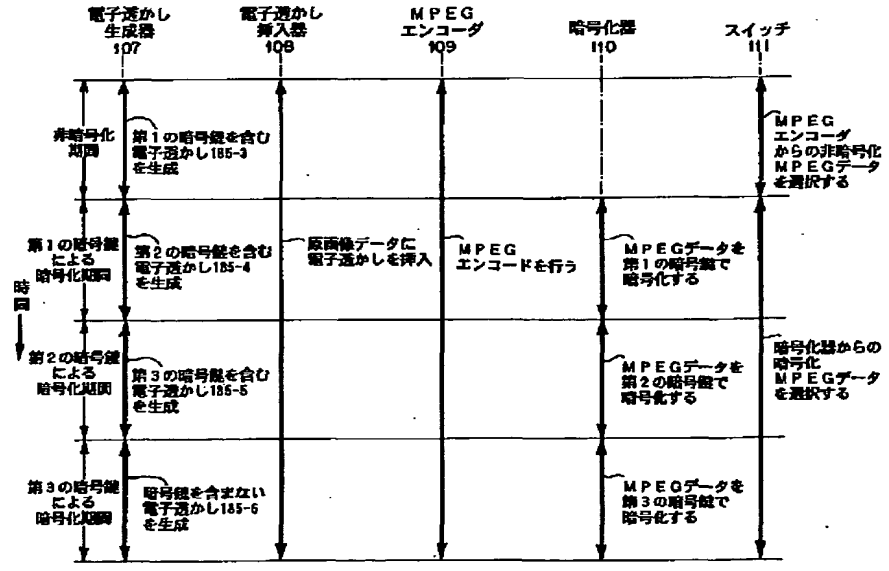
【図８】


非暗号化期間
第１の暗号鍵による暗号化期間
第２の暗号鍵による暗号化期間
第３の暗号鍵による暗号化期間
原画像データ 181
電子透かし挿入済画像データ 182
1 1 X X X X X X (Binary)
第１の暗号鍵
世代管理情報ビット
185-3
1 1 X X X X X X (Binary)
第２の暗号鍵
世代管理情報ビット
185-4
1 1 X X X X X (Binary)
第３の暗号鍵
世代管理情報ビット
185-5
1 1 0 0 0 0 0 0 (Binary)
任意値
世代管理情報ビット
185-6
非暗号化MPEGデータ 183
一部が暗号化されたMPEGデータ 184
184-3
暗号化されていないMPEGデータ
184-4
第１の暗号鍵により暗号化されたMPEGデータ
184-5
第２の暗号鍵により暗号化されたMPEGデータ
184-6
第３の暗号鍵により暗号化されたMPEGデータ

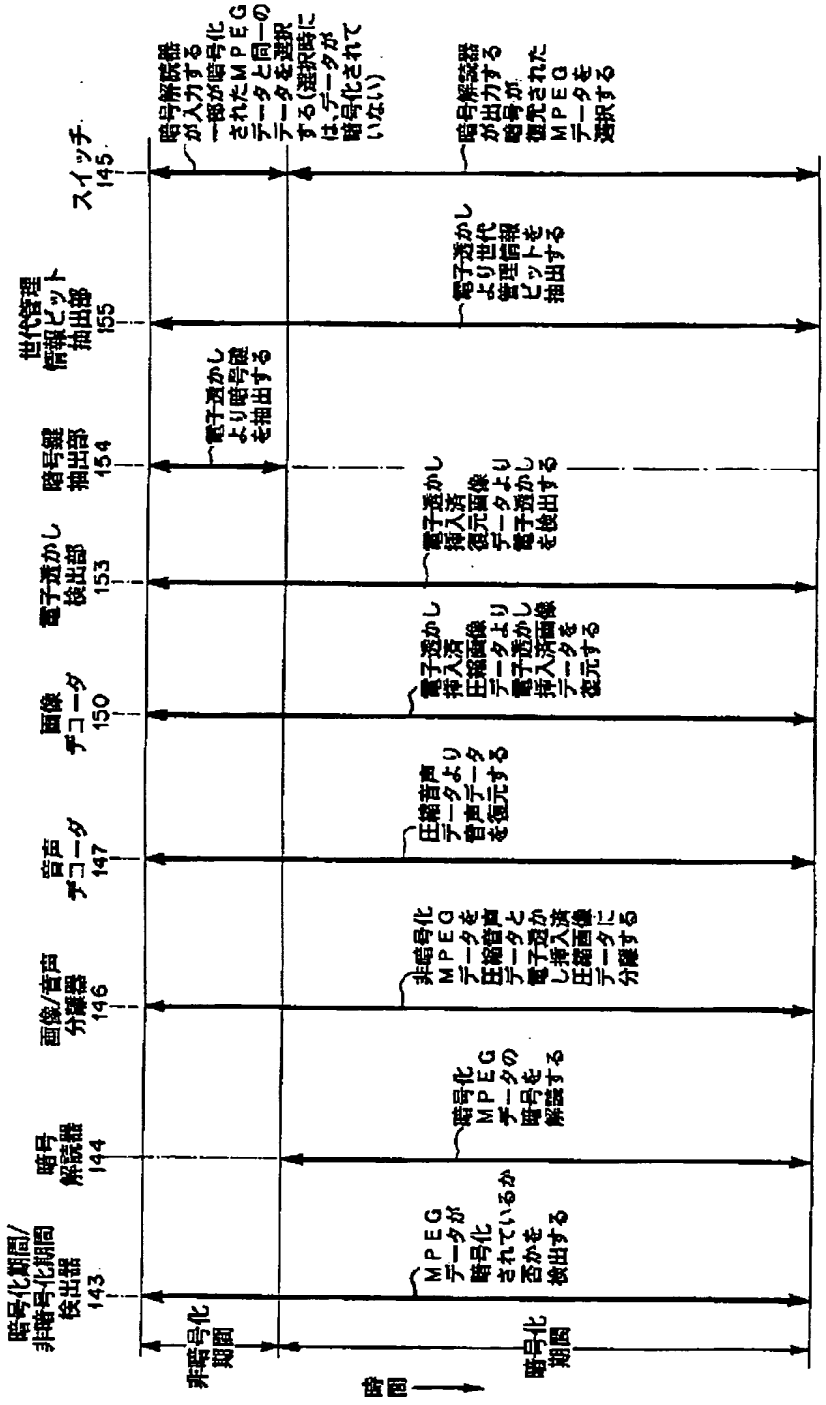
【図６】


電子透かし
生成器
107
電子透かし
挿入器
108
MPEG
エンコーダ
109
暗号化器
110
スイッチ
111
非暗号化
期間
暗号鍵を含む
電子透かし185-1
を生成
MPEGエンコーダ
からの非暗号化
MPEGデータ
を選択する
時間
原画像データに
電子透かしを挿入
MPEG
エンコード
を行う
暗号化
期間
暗号鍵を含まない
電子透かし185-2
を生成
MPEGデータ
を暗号鍵で
暗号化する
暗号化器からの
暗号化MPEG
データを選択する

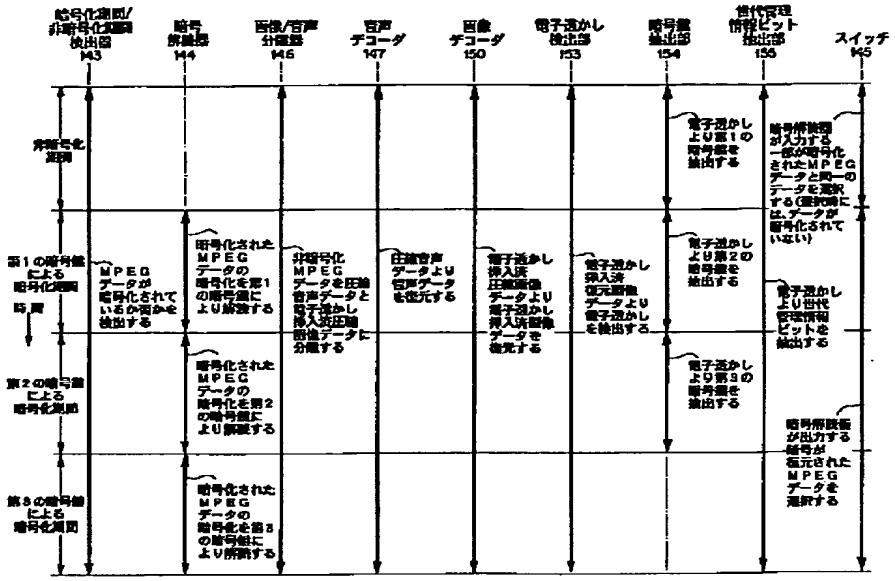
【図９】


電子透かし
生成器
107
電子透かし
挿入器
108
MPEG
エンコーダ
109
暗号化器
110
スイッチ
111
非暗号化
期間
第１の暗号鍵を含む
電子透かし185-3
を生成
MPEG
エンコーダ
からの非暗号化
MPEGデータ
を選択する
第１の暗号鍵
による
暗号化期間
第２の暗号鍵を含む
電子透かし185-4
を生成
原画像データに
電子透かしを挿入
MPEG
エンコードを行う
MPEGデータを
第１の暗号鍵で
暗号化する
時間
第２の暗号鍵
による
暗号化期間
第３の暗号鍵を含む
電子透かし185-5
を生成
MPEGデータを
第２の暗号鍵で
暗号化する
暗号化器からの
暗号化
MPEGデータ
を選択する
第３の暗号鍵
による
暗号化期間
暗号鍵を含まない
電子透かし185-6
を生成
MPEGデータを
第３の暗号鍵で
暗号化する

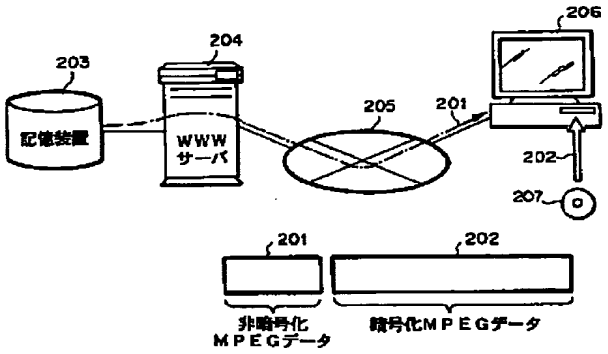
【図７】


暗号化期間/非暗号化期間検出器 143
暗号解読器 144
画像/音声分離器 146
音声デコーダ 147
画像デコーダ 150
電子透かし検出部 153
暗号鍵抽出部 154
世代管理情報ビット抽出部 155
スイッチ 145
MPEGデータが暗号化されているか否かを検出する
暗号化MPEGデータの暗号を解読する
非暗号化MPEGデータを圧縮音声データと電子透かし挿入済圧縮画像データに分離する
圧縮音声データより音声データを復元する
電子透かし挿入済圧縮画像データより電子透かし挿入済画像データを復元する
電子透かし挿入済復元画像データより電子透かしを検出する
電子透かしより暗号鍵を抽出する
電子透かしより世代管理情報ビットを抽出する
暗号解読器が入力する一部が暗号化されたMPEGデータと同一のデータを選択する(選択時にはデータが暗号化されていない)
暗号解読器が出力する暗号が復元されたMPEGデータを選択する
非暗号化期間
暗号化期間
時間

【図１０】



【図１１】



フロントページの続き

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｇ１１Ｂ	20/10		Ｇ１０Ｌ	9/00	Ｅ　５Ｄ０４５
Ｈ０４Ｎ	1/387				Ｎ　５Ｊ１０４
	7/08			9/18	Ｍ
	7/081		Ｈ０４Ｎ	7/08	Ｚ
	7/167			7/167	Ｚ

Ｆターム(参考) 5B057 CA08 CA12 CA16 CB08 CB12
CB16 CC01 CE08
5C063 AB03 AC01 AC05 DA07 DA13
DB09
5C064 CA14 CB01 CC04 CC06
5C076 AA14 BA06
5D044 AB05 AB07 BC03 CC06 DE12
DE50 EF05 FG18 GK08 GK17
GK20 HL11
5D045 DA20
5J104 AA14 NA02